DETAILED ACTION

This final action is in response to the amendment filed on 02/26/2008. In light of the applicant's amendments and remarks, the examiner hereby withdraws his previous Specification Objection and 35 U.S.C. 112 2nd paragraph rejections. The examiner notes that additional explanations/notes have been added to the 35 U.S.C. 103(a) rejections below for the purposes of clarity. Claims 1-62 are pending and have been considered as follows.

Specification

1. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

- Claims 12 & 61 recite "a computer-readable medium" however, the applicant's Specification never recites this.
- The examiner notes that the applicant's Specification only ever recites "memory" and other specific types of memory on pages 13-14.

Claim Objections

2. Claims 11, 12, 26, 61, & 62 are objected to because of the following informalities:

- Claims 11, 12, 26, 61, & 62 line 1 recite "for" which should be "…configured to…";

Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 11, 12, 13-17, 26-32, & 41-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ahn et al. (US-6160627-A).

Claim 1:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, but do not explicitly disclose,

- "receiving training symbols transmitted from a QKD transmitter over a QKD path," although Ahn et al. do suggest receiving a signal/transmission wavelength involving an interferometer over an optical fiber, as recited below;
- "controlling a length of the QKD path based on the received training symbols," although Ahn et al. do suggest a stabilized optical fiber interferometer controlling transmission wave length, as recited below;

however, they do disclose,

- "FIG. 1 illustrates a stabilized optical fiber Mach-Zehnder interferometer in which a transmission wavelength is controlled according to the present invention" [column 3 lines 6-8];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "receiving training symbols transmitted from a QKD transmitter over a QKD path" and "controlling a length of the QKD path based on the received training symbols," in the invention as disclosed by Ahn et al. since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 11:

Ahn et al. disclose a system for automatically initializing a length of a quantum cryptographic key distribution (QKD) path in a QKD system, but do not explicitly disclose,

- "a QKD receiver configured to receive training symbols from a QKD transmitter over the QKD path," although Ahn et al. do suggest receiving a signal/transmission wavelength involving an interferometer over an optical fiber, as recited below;
- "a phase shifting element disposed on the QKD path," although Ahn et al. do suggest a phase modulator, as recited below;

- "processing logic configured to automatically initialize the length of the QKD path, using the phase shifting element, based on the received training symbols," although Ahn et al. do suggest varying the length of the optical fiber, as recited below;

however, they do disclose,

- "FIG. 1 illustrates a stabilized optical fiber Mach-Zehnder interferometer in which a transmission wavelength is controlled according to the present invention" [column 3 lines 6-8];
- "an optical fiber phase modulator (fiber stretcher)" [column 3 lines 17-18];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a QKD receiver configured to receive training symbols from a QKD transmitter over the QKD path" and "a phase shifting element disposed on the QKD path" and "processing logic configured to automatically initialize the length of the QKD path, using the phase shifting element, based on the received training symbols," in the invention as disclosed by Ahn et al. since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 12:

Ahn et al. disclose a computer-readable medium containing instructions for controlling at least one processor to perform a method of controlling path length in a quantum cryptographic key distribution (QKD) system, but do not explicitly disclose,

- "receiving symbols transmitted from a QKD transmitter over a QKD path," although Ahn et al. do suggest receiving a signal/transmission wavelength involving an interferometer over an optical fiber, as recited below;
- "controlling a length of the QKD path based on the received symbols," although Ahn et al. do suggest varying the length of the optical fiber, as recited below;

however, they do disclose,

- "FIG. 1 illustrates a stabilized optical fiber Mach-Zehnder interferometer in which a transmission wavelength is controlled according to the present invention" [column 3 lines 6-8];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "receiving symbols transmitted from a QKD transmitter over a QKD path" and "controlling a length of the QKD path based on the received symbols," in the invention as disclosed by Ahn et al. since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which

utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 13:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, but do not explicitly disclose,

- "employing a phase shifting element in the second interferometer," although Ahn et al. do suggest a phase modulator, as recited below;
- "automatically adjusting the phase shifting element to control the path length based on symbols transmitted over the path," although Ahn et al. do suggest varying the length of the optical fiber, as recited below;

however, they do disclose,

- "an optical fiber phase modulator (fiber stretcher)" [column 3 lines 17-18];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "employing a phase shifting element in the second interferometer" and "automatically adjusting the phase shifting element to control the path length based on symbols transmitted over the path," in the invention as disclosed by Ahn et al. since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics).

Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 14:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 13 above, further comprising,

- "the phase shifting element comprises a fiber stretcher" (i.e. "an optical fiber phase modulator (fiber stretcher)" [column 3 lines 17-18].

Claim 15:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 14 above, further comprising,

- "adjusting a voltage applied to the fiber stretcher based on the symbols transmitted over the path" (i.e. "an optical fiber phase modulator (fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers" [column 3 lines 17-19].

Claim 16:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 13 above, further comprising,

- "the phase shifting element comprises a phase modulator" (i.e. "an optical fiber phase modulator (fiber stretcher)" [column 3 lines 17-18].

Claim 17:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 16 above, further comprising,

- "adjusting a voltage applied to the phase modulator based on the symbols transmitted over the path" (i.e. "an optical fiber phase modulator (fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers" [column 3 lines 17-19].

Claim 26:

Ahn et al. disclose a system for automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, but do not explicitly disclose,

- "a QKD path including a first interferometer and a second interferometer," although Ahn et al. do suggest an interferometer at both ends of a fiber optic communications, as recited below;
- "a phase shifting element disposed in at least one of the first and second interferometers," although Ahn et al. do suggest a phase modulator, as recited below;

- "processing logic configured to automatically adjust the phase shifting element to control a length of the path," although Ahn et al. do suggest varying the length of the optical fiber, as recited below;

however, they do disclose,

- "The optical fiber Mach-Zehnder interferometer filter according to the present invention includes a 1.3 .mu.m wavelength turnable laser diode (TLD) 10 (or DFB-LD(Distributed Feedback laser diode)) for implementing a stabilization of an interferometer, first and second 3 dB optical fiber couplers" [column 3 lines 9-14];
- "an optical fiber phase modulator (fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers" [column 3 lines 17-19];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a QKD path including a first interferometer and a second interferometer" and "a phase shifting element disposed in at least one of the first and second interferometers" and "processing logic configured to automatically adjust the phase shifting element to control a length of the path," in the invention as disclosed by Ahn et al. since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications

medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 27:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, but do not explicitly disclose,

- "employing a feedback system in the QKD system," although Ahn et al. do suggest feedback to a phase modulator, as recited below;
- "where the OKD system comprises a first interferometer and a second interferometer," although Ahn et al. do suggest an interferometer at both end of a fiber optic communications, as recited below;
- "automatically controlling the path length, using the feedback system, based on symbols transmitted over the path from the first interferometer to the second interferometer," although Ahn et al. do suggest varying the length of an optical fiber, as recited below;

however, they do disclose,

- "feeding-back to the optical fiber phase modulator" [column 3 lines 31-32];
- "The optical fiber Mach-Zehnder interferometer filter according to the present invention includes a 1.3 .mu.m wavelength turnable laser diode (TLD) 10 (or DFB-LD(Distributed Feedback laser diode)) for implementing a stabilization of an interferometer, first and second 3 dB optical fiber couplers" [column 3 lines 9-14];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "employing a feedback system in the QKD system" and "automatically controlling the path length, using the feedback system, based on symbols transmitted over the path," in the invention as disclosed by Ahn et al. since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 28:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 27 above, further comprising,

- "the feedback system comprises a phase shifting element" (i.e. "an optical fiber phase modulator (fiber stretcher)") [column 3 lines 17-18].

Claim 29:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 28 above, further comprising,

- "the phase shifting element comprises a fiber stretcher" (i.e. "an optical fiber phase modulator (fiber stretcher)") [column 3 lines 17-18].

Claim 30:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 29 above, further comprising,

- "adjusting a voltage applied to the fiber stretcher based on the symbols transmitted over the path" (i.e. "an optical fiber phase modulator (fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers" [column 3 lines 17-19].

Claim 31:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 28 above, further comprising,

- "the phase shifting element comprises a phase modulator" (i.e. "an optical fiber phase modulator (fiber stretcher)") [column 3 lines 17-18].

Claim 32:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 31 above, further comprising,

- "adjusting a voltage applied to the phase modulator based on the symbols transmitted over the path" (i.e. "an optical fiber phase modulator(fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers" [column 3 lines 17-19].

Claim 41:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, but do not explicitly disclose,

- "a QKD receiver configured to receive symbols transmitted over a QKD path," although Ahn et al. do suggest receiving a signal/transmission wavelength involving an interferometer over an optical fiber, as recited below;
- "a feedback system configured to control a length of the QKD path based on the received symbols," although Ahn et al. do suggest varying the length of an optical fiber, as recited below;

however, they do disclose,

- "FIG. 1 illustrates a stabilized optical fiber Mach-Zehnder interferometer in which a transmission wavelength is controlled according to the present invention" [column 3 lines 6-8];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a QKD receiver configured to receive symbols transmitted over a QKD path" and "a feedback system configured to control a length of the QKD path based on the received symbols," in the invention as disclosed by Ahn et al. since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to

any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 42:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 41 above, further comprising,

- "the feedback system comprises a phase shifting element" (i.e. "an optical fiber phase modulator (fiber stretcher)") [column 3 lines 17-18].

Claim 43:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 42 above, further comprising,

- "the phase shifting element comprises a fiber stretcher" (i.e. "an optical fiber phase modulator (fiber stretcher)") [column 3 lines 17-18].

Claim 44:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 42 above, further comprising,

- "the phase shifting element comprises a phase modulator" (i.e. "an optical fiber phase modulator (fiber stretcher)") [column 3 lines 17-18].

5. Claims 52-59, 61 & 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Page (US-5157461-A).

Claim 52:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, but does not explicitly disclose,

- "determining probabilities associated with a plurality of detection events," although Page does suggest error computation and statistical effects of residual noise, as recited below;
- "the plurality of detection events being associated with a sequence of symbols received over the path in the QKD system," although Page does suggest a detection circuit responsive to a signal, as recited below;
- "controlling the length of the path based on the determined probabilities," although Page does suggest utilizing a Kalman filter to provide optimal estimation techniques for a signal, as recited below;

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];
- "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation" [column 26 lines 43-46];

- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "determining probabilities associated with a plurality of detection events" and "the plurality of detection events being associated with a sequence of symbols received over the path in the QKD system" and "controlling the length of the path based on the determined probabilities," in the invention as disclosed by <u>Page</u> since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 53:

<u>Page</u> discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 52 above, further comprising,

- "the probabilities comprise conditional probabilities" (i.e. "the statistical effects of the previously-described residual noise") [column 18 lines 23-24].

Claim 54:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 52 above, further comprising,

- "estimating a phase error based on the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise") [column 18 lines 20-24].

Claim 55:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 54 above, further comprising,

- "controlling the path length of the QKD path further based on the estimated phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55].

Claim 56:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 54 above, further comprising,

- "performing a least squares estimation of the phase error using the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise") [column 18 lines 20-24].

Claim 57:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 54 above, further comprising,

- “employing at least one Kalman filter to estimate the phase error” (i.e. “a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location” [column 17 lines 51-55].

Claim 58:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 54 above, further comprising,

- “performing a robust least squares estimation of the phase error using the determined probabilities” (i.e. “a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location” [column 17 lines 51-55].

Claim 59:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 58 above, further comprising,

- “at least one of least absolute residuals and Bisquare weight” (i.e. “These detections can be accomplished by means of conventional methods such as "curve fitting" utilizing the principles of "linear least squares" as commonly known in the art”) [column 16 lines 51-54].

Claims 61 & 62:

Page discloses a computer-readable medium containing instructions for controlling at least one processor to perform a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system and a system for controlling a length of a path in a quantum cryptographic key distribution (QKD) system, but does not explicitly disclose,

- "(means for) determining probabilities associated with a plurality of detection events," although Page does suggest estimation error computations and statistical effects of residual noise, as recited below;
- "the plurality of detection events being associated with a sequence of symbols received over the path in the QKD system," although Page does suggest a detection circuit responsive to a signal, as recited below;
- "(means for) controlling the length of the path based on the determined probabilities," although Page does suggest utilizing curve fitting or least linear squares methods, as recited below;

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];
- "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation" [column 26 lines 43-46];

- “These detections can be accomplished by means of conventional methods such as "curve fitting" utilizing the principles of "linear least squares" as commonly known in the art” [column 16 lines 51-54];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant’s invention to include, “determining probabilities associated with a plurality of detection events” and “the plurality of detection events being associated with a sequence of symbols received over the path in the QKD system” and “controlling the length of the path based on the determined probabilities,” in the invention as disclosed by Page since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant’s claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

6. Claims 2-10, 18-25, 33-40, 45-51, & 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ahn et al. (US-6160627-A) in view of Page (US-5157461-A).

Claim 2:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 1 above, but do not disclose,

- "estimating a phase error associated with transmission of the training symbols over the QKD path," although Page does suggest estimation error computations, as recited below;

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "estimating a phase error associated with transmission of the training symbols over the QKD path," in the invention as disclosed by Ahn et al. for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 3:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 2 above, further comprising,

- "determining probabilities of detection events associated with the received training symbols" (i.e. "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation") [column 26 lines 43-46].

Claim 4:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 3 above, further comprising,

- "estimating the phase error based on the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise") [column 18 lines 20-24].

Claim 5:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 2 above, further comprising,

- "controlling the length of the QKD path based on the estimated phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 6:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 4 above, further comprising,

- "controlling the length of the QKD path based on the estimated phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 7:

<u>Ahn et al.</u> disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 4 above, further comprising,

- "performing a least squares estimation of the phase error using the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise") [column 18 lines 20-24].

Claim 8:

<u>Ahn et al.</u> disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 2 above, further comprising,

- "employing at least one Kalman filter to estimate the phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 9:

<u>Ahn et al.</u> disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 4 above, further comprising,

- "performing a robust least squares estimation of the phase error using the determined probabilities" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 10:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 9 above, further comprising,

- "at least one of least absolute residuals and Bisquare weights" (i.e. "These detections can be accomplished by means of conventional methods such as "curve fitting" utilizing the principles of "linear least squares" as commonly known in the art") [column 16 lines 51-54].

Claim 18:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 13 above, but do not disclose,

- "estimating a phase error associated with symbols transmitted over the path," although Page does suggest estimation error computations, as recited below;

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "estimating a phase error associated with symbols transmitted over the path," in the invention as disclosed by Ahn et al. for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 19:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 18 above, further comprising,

- "determining probabilities of detection events associated with the symbols transmitted over the path" (i.e. "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation") [column 26 lines 43-46].

Claim 20:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 19 above, further comprising,

- "estimating the phase error based on the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24].

Claim 21:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 18 above, further comprising,

- "the phase shifting element is automatically adjusted to control the path length further based on the estimated phase error" (i.e. "a sequential Kalman filter can provide optimal

estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55].

Claim 22:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 20 above, further comprising,

- "performing a least squares estimation of the phase error using the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24].

Claim 23:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 18 above, further comprising,

- "employing at least one Kalman filter to estimate the phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55].

Claim 24:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 20 above, further comprising,

- "performing a robust least squares estimation of the phase error using the determined probabilities" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55].

Claim 25:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 24 above, further comprising,

- "at least one of least absolute residuals and Bisquare weights" (i.e. "These detections can be accomplished by means of conventional methods such as "curve fitting" utilizing the principles of "linear least squares" as commonly known in the art") [column 16 lines 51-54].

Claim 33:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 27 above, but do not disclose,

- "estimating a phase error associated with symbols transmitted over the path," although Page does suggest estimation error computations, as recited below;

however, Page does disclose,

- “an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise” [column 18 lines 20-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant’s invention to include, “estimating a phase error associated with symbols transmitted over the path,” in the invention as disclosed by Ahn et al. for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 34:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 33 above, further comprising,

- “determining probabilities of detection events associated with the symbols transmitted over the path” (i.e. “the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation”) [column 26 lines 43-46].

Claim 35:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 34 above, further comprising,

- “estimating the phase error based on the determined probabilities” (i.e. “an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise”) [column 18 lines 20-24].

Claim 36:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 33 above, further comprising,

- "the path length is automatically controlled further based on the estimated phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 37:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 35 above, further comprising,

- "performing a least squares estimation of the phase error using the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise") [column 18 lines 20-24].

Claim 38:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 35 above, further comprising,

- "employing at least one Kalman filter to estimate the phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 39:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 35 above, further comprising,

- "performing a robust least squares estimation of the phase error using the determined probabilities" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 40:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 39 above, further comprising,

- "at least one of least absolute residuals and Bisquare weights" (i.e. "These detections can be accomplished by means of conventional methods such as "curve fitting" utilizing the principles of "linear least squares" as commonly known in the art") [column 16 lines 51-54].

Claim 45:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 41 above, but do not disclose,

- "estimate a phase error associated with the symbols transmitted over the QKD path based on the received symbols," although Page does suggest estimation error computations, as recited below;

however, Page does disclose,

- “an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise” [column 18 lines 20-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant’s invention to include, “estimate a phase error associated with the symbols transmitted over the QKD path based on the received symbols,” in the invention as disclosed by Ahn et al. for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 46:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 45 above, further comprising,

- “determine probabilities of detection events associated with the symbols transmitted over the QKD path” (i.e. “the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation”) [column 26 lines 43-46].

Claim 47:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 46 above, further comprising,

- “estimate the phase error based on the determined probabilities” (i.e. “an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise”) [column 18 lines 20-24].

Claim 48:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 45 above, further comprising,

- "the estimation system comprises a least squares estimator" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 49:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 45 above, further comprising,

- "the estimation system comprises at least one Kalman filter" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 50:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 45 above, further comprising,

- "estimation system comprises a robust least squares estimator" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 51:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 50 above, further comprising,

- “the robust least squares estimator employs at least one of least absolute residuals and Bisquare weights” (i.e. “These detections can be accomplished by means of conventional methods such as "curve fitting" utilizing the principles of "linear least squares" as commonly known in the art”) [column 16 lines 51-54].

Claim 60:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint comprising,

- “a QKD receiver configured to receive a sequence of symbols transmitted over a QKD path” (i.e. “FIG. 1 illustrates a stabilized optical fiber Mach-Zehnder interferometer in which a transmission wavelength is controlled according to the present invention”) [column 3 lines 6-8];
- “a phase shifting element disposed on the QKD path” (i.e. “an optical fiber phase modulator (fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers”) [column 3 lines 17-19];

but do not disclose,

- “processing logic configured to: determine conditional probabilities associated with a plurality of detection events,” although Page does suggest error computations and statistical effects of residual noise, as recited below;
- “the plurality of detection events being associated with the sequence of symbols,” although Page does suggest a detection circuit responsive to a signal, as recited below;

- “processing logic configured to: adjust the phase shifting element to control a length of the QKD path based on the determined conditional probabilities,” although Page does suggest utilizing a Kalman filter to provide optimal estimation techniques for a signal, as recited below;

however, Page does disclose,

- “an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise” [column 18 lines 20-24];
- “the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation” [column 26 lines 43-46];
- “a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location” [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant’s invention to include, “processing logic configured to: determine conditional probabilities associated with a plurality of detection events” and “the plurality of detection events being associated with the sequence of symbols” and “processing logic configured to: adjust the phase shifting element to control a length of the QKD path based on the determined conditional probabilities,” in the invention as disclosed by Ahn et al. for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Response to Arguments

7. Applicant's arguments filed 02/26/2008 have been fully considered but they are not persuasive.

- The applicant's arguments regarding Claims 1, 11, & 12 and their dependents that recite, "AHN does not disclose or suggest anything that could even remotely be interpreted as receiving training symbols" and "AHN also does not disclose or suggest a quantum cryptographic key distribution system" and "AHN cannot disclose or suggest receiving training symbols transmitted from a QKD transmitter over a QKD path" and "AHN cannot disclose or suggest controlling a length of a OKD path based on the received training symbols," have been carefully considered but are non-persuasive.
    - The examiner notes that the examiner interpreted "receiving training symbols" as receiving an optical signal having a wavelength.
    - The examiner contends that the prior art of record as of the first Non-Final office action did not explicitly recite "a quantum cryptographic key distribution system," however, upon consideration of the applicant's claims, it appeared to the examiner that the applicant's invention is directed to "controlling path length," thus, when giving the broadest most reasonable interpretation, the examiner found that the applicant's claim language was broad enough to encompass other fiber optic communications systems and not just a QKD system exclusively.

  - o The examiner interpreted the QKD path as a fiber optic communications path.
  - o The examiner interpreted the “controlling a length of a path based on the received symbols” as the controlling of the wavelength/phase/polarization of the received light signal.

- The applicant’s arguments regarding Claims 13 & 26 and their dependents that recite, “AHN does not disclose or suggest a second interferometer” and “AHN cannot disclose or suggest employing a phase shifting element in a second interferometer” and “AHN also does not disclose or suggest automatically adjusting a phase shifting element to control the path length based on symbols transmitted over a path (where the path comprises a first interferometer and a second interferometer)” and “AHN does not disclose or suggest adjusting a voltage applied to a phase modulator based on the symbols transmitted over the path,” have been carefully considered but are non-persuasive.
  - o The examiner notes that AHN does suggest at least one interferometer, and it would have been reasonable to expect that the phase shifting and path length control applied to one interferometer would be the same for another interferometer.
  - o The examiner also notes that AHN does suggest phase modulation of a signal which would involve voltage adjustment(s);

- The applicant's arguments regarding Claims 27 & 41 and their dependents that recite, "AHN does not disclose or suggest employing a feedback system in the QKD system, where the QKD system comprises a first interferometer and a second interferometer, and automatically controlling the path length, using the feedback system, based on symbols transmitted over the path from the first interferometer to the second interferometer," have been carefully considered but are non-persuasive.
    - The examiner notes that AHN does suggest a feedback system, utilizing at least one interferometer for path length control of an optical signal over a fiber optic communications medium;
- The applicant's arguments regarding Claims 52, 61, & 62 and their dependents that recite, "PAGE does not disclose determining probabilities associated with a plurality of detection events, the plurality of detection events being associated with a sequence of symbols received over a path in the QKD system and controlling a length of the path based on the determined probabilities," have been carefully considered but are non-persuasive.
    - The examiner notes that PAGE does suggest error computations and statistical effects in terms of the probabilities; a detection circuit detecting aspects of a signal, suggesting the detection of specific elements in a signal; and utilizing a Kalman filter for error control, resulting in path length control;

- The applicant's arguments regarding the Examiner's motivation that states, "Applicants submit that the Examiner's allegation is merely a conclusory statement," has been carefully considered but is non-persuasive.
  - The examiner notes that the motivational statements provided have been provided in light of the prior art of record or that which is considered old and well known in the art of optical communications or what would have been reasonable to expect one of ordinary skill in the art to attempt/try within the confines of the laws of physics and the functionalities of optical communications assuming the art area of quantum cryptography and optical communications.
- The applicant's arguments regarding the Examiner's motivation that states, "PAGE does not disclose or suggest that a robust least squares estimation comprises at least one of least absolute residuals and Bisquare weights," has been carefully considered but is non-persuasive.
  - The examiner notes that PAGE does suggest the usage of alternative estimation computations for residuals namely, a Kalman filter.

8. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure is presented below by the examiner for the purposes of consideration by the applicant.

a. <u>Galindo et al.</u> ("Information and computation: Classical and quantum aspects") – interferometry, phase shifting, quantum mechanics, probabilistic, pathways;

b. Merolla et al. ("Quantum cryptographic device using single-photon phase modulation") – interferometer(s), constructive/destructive interference, path length control;

c. Tittel et al. ("Quantum Cryptography Using Entangled Photons in Energy-Time Bell States") – Quantum Key Distribution (QKD), interferometer(s), phase, path length;

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
06/10/2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136